PROTECTIVE CIRCUIT FOR PROTECTING HARD DISK DATA

FIELD OF THE INVENTION

This invention relates generally to protective circuits for protecting data, particularly to a protective circuit for protecting hard disk data arranged between a Hard Disk Drive (HDD) and the motherboard in the form like an Integrated Drive Electronics (IDE) interface.

BACKGROUND OF THE INVENTION

A protective circuit for protecting hard disk data is usually made in the form of an interface card and plugged in an Industry Standard Architecture (ISA) slot or a Peripheral Component Interconnect (PCI) slot. The measure of the protective circuit is more or less concerned with the operating system (O/S) set in a hard disk and is mostly limited in intercepting the interruption instruction INT **13** of the widely known Basic Input/Output System (BIOS) chip(s) lying on the motherboard for operating a Hard Disk Drive (HDD). Therefore, a protective circuit based on Microsoft operating system may not be compatible with that of Apple series, namely, the protective measure is somewhat dependent on an operating system. Besides, a user has to install a related driver in addition to a conventional protective circuit, which cannot function anymore when the driver is damaged or disabled.

SUMMARY OF THE INVENTION

The primary object of this invention is to provide a protective circuit for protecting hard disk data, which is located between a motherboard and a hard disk (HD) drive and is irrespective of any operating system or driving program.

The protective circuit should comprise:

a first HD coupling device connected to a hard disk port of a motherboard;

a second HD coupling device connected to a hard disk;

a HD signal processor coupled to: the first HD coupling device, the second HD coupling device, and a microprocessor;

a random access memory (RAM) connected to the microprocessor;

a nonvolatile semiconductor memory having program codes for switching a read/write instruction of the hard disk port on the motherboard with respect to the hard disk from a main data space to a virtual data space thereof; and

the microprocessor for running the program codes.

In case the data stored in the virtual data space are damaged, the protective circuit of this invention can be applied to recopy the data in the main data space to the virtual data space to revive the latter.

For more detailed information regarding this invention together with advantages or features thereof, at least an example of preferred embodiment will be elucidated below with reference to the annexed drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

The related drawings in connection with the detailed description of this invention, which is to be made later, are described briefly as follows, in which:

FIG. **1** shows the architecture of this invention;

FIG. **2** is a schematic view showing that a hard disk is partitioned into a main and a virtual data space;

FIG. **3** shows a menu of running an external program code; and

FIG. **4** is a flowchart for infusing the program code of this invention into a nonvolatile semiconductor memory.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Based on the architecture of this invention shown in FIG. **1**, a protective circuit for protecting hard disk (HD) data **10** comprises a first HD coupling device **100**, a second HD coupling device **101**, a HD signal processor **103**, a random access memory (RAM) **105**, a programmed nonvolatile semiconductor memory **102**, and a microprocessor **104**. The first HD coupling device **100** is connected with a hard disk port **20**a on a motherboard **20** while the second HD coupling device **101** is connected with a hard disk (HD) **30**. The HD signal processor **103** is the hub connected with the first and the second HD coupling devices **100**, **101**, as well as the microprocessor **104** respectively. And moreover, the RAM **105** is coupled to the microprocessor **104**.

The microprocessor **104** is to run a program code in the semiconductor memory **102** to convert a read/write command for access of a main data space in the HD **30** into a virtual data space.

An Integrated Drive Electronics (IDE) interface is generally disposed on a conventional motherboard **20** for jointing with an IDE hard disk drive or a CD ROM drive. In a preferred embodiment of the protective circuit **10** of this invention, both the first and the second HD coupling devices **100**, **101** are IDE couplings and connected to the hard disk port **20**a on the motherboard **20** and to the HD **30** through a ribbon cable **40**a, **40**b respectively.

According to the protective circuit **10**, the HD **30** must be partitioned in advance into a main and a virtual data space **30**a, **30**b as shown in FIG. **2**. The main data space **30**a and the virtual data space **30**b are two HD spaces equal to L with respect to an initial address S0, S1, wherein the magnitude of space L and the data space **30**a, **30**b can be defined or partitioned by running an external program code. As shown in FIG. **3**, when a user chooses item **1** to key in 1000, the HD **30** is partitioned into a main and a virtual data space **30**a, **30**b in 1000 MB equally, wherein the main data space **30**a is used to store an installed bulky software like the Microsoft Window operating System, maybe plus the Microsoft Office application software. The user may choose item **2**—setup mode at the first time—for installing operating system and application software to the main data space **30**a After completion of the setup job, he may now choose item **3** to enter a virtual-data-space switching mode, and the protective circuit **10** would switch and copy all the data stored in the main data space **30**a to the virtual data space **30**b, so that all the read/write requests afterwards are allowed to access the virtual data space **30**b instead, and thereby protect the operating system and application software stored in the main data space **30**a.

Such a switch-measure has built a firewall surrounding the main data space **30**a to allow virus to invade the virtual data space **30**b only. In the case of virus invasion, a user may resume FIG. **3** and enter item **3** again, the protective circuit **10** would recopy all the data in the main data space **30**a to the virtual data space **30**b one more time and rebuild the operating system and application software in the latter. Moreover, a remaining space **30**c, if any, in the partitioned HD **30** is treated as a logic HD to the operating system.